REMARKS

Claims are being amended for better clarity. If the Examiner has questions regarding this case, the Examiner is invited to contact Applicants' undersigned representative at the telephone number listed below.

Respectfully submitted,
Mark Moriconi, et al.

Date: 7/26/02

By: _____

Eppa Hite, Reg. No. 30,266
Carr & Ferrell *LLP*
2225 East Bayshore Road, Suite 200
Palo Alto, CA 94303
Phone (650) 812-3428
Fax (650) 812-3444

VERSION MARKED UP TO SHOW CHANGES BEING MADE

29. (Twice amended) A system for controlling user access in a distributed computing environment, comprising:

a global policy specifying access privileges of the user to securable components;

a policy manager located on a server for managing and distributing to a client a local client policy based on the global policy [to a client], and

an application guard located on the client for managing access to the securable components as specified by the local client policy;

wherein the application guard further allows for additional customized code to process and evaluate authorization requests based on the additional customized code.

69. (Amended) A method for maintaining security in a distributed computing environment, comprising:

managing a security policy via a policy manager; and

managing, via an application guard, access to securable components as specified by the security policy;

wherein the application guard further allows for additional customized code to process and evaluate authorization requests based on the additional customized code.

70. (Amended) A method for controlling user access via a system in a distributed computing environment, comprising:

specifying via a global policy [access] privileges of the user [via a global policy] to access securable components;

managing and distributing, via a policy manager, to a client, a local client policy based on the global policy [located on a server to a client], and

managing, [access] via an application guard located on the client, access to the securable components as specified by the local client policy;

wherein the application guard further allows for additional customized code to process and evaluate authorization requests based on the additional customized code.

71. (Amended) A method for authorization that provides for a user access to securable components of a system [for a user], comprising:

specifying via a policy [access] privileges of the user [via a policy] to access the securable components;

managing [access] via an application guard access to the securable components; and

executing the application guard via a processor coupled to the [said] system [said application guard];

wherein the application guard further allows for additional customized code to process and evaluate authorization requests based on the additional customized code.

79. (Amended) A method for providing a system for controlling user access in a distributed computing environment, comprising:

providing a global policy specifying [access] privileges of the user to access securable components;

providing a policy manager located on a server for managing and distributing to a client a local client policy based on the global policy [to a client], and

providing an application guard located on the client for managing access to the securable components as specified by the local client policy;

wherein the application guard further allows for additional customized code to process and evaluate authorization requests based on the additional customized code.